РОСНЕФТЬ
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
НЕФТЯНАЯ КОМПАНИЯ

APPROVED
Resolution of the Board of Directors of
Rosneft Oil Company
"31" March 2020
Minutes dated "03" April 2020
№ 19
Enacted on "21" April 2020 by the order of
Rosneft Oil Company
No. 233 dd. "21" April 2020

COMPANY POLICY

INFORMATION SECURITY

№ П3-11.01 П-01

VERSION 2.00

MOSCOW
2020

TABLE OF CONTENTS

1. INTRODUCTORY PROVISIONS 3
PURPOSE 3
SCOPE OF APPLICATION 3
VALIDITY AND AMENDMENT PROCEDURE 3
2. GLOSSARY 4
2.1. CORPORATE GLOSSARY TERMS AND DEFINITIONS 4
2.2. ROLES 5
3. INFORMATION SECURITY POLICY STATEMENT 7
3.1. COMPANY'S GOALS AND OBJECTIVES RELATED TO INFORMATION SECURITY 8
3.2. INFORMATION SECURITY OBJECTS 8
3.3. MAIN PRINCIPLES OF INFORMATION SECURITY MANAGEMENT AND ASSURANCE 9
4. LIABILITY FOR BREACHES of INFORMATION SECURITY 12
5. AWARENESS AND COMMUNICATION OF POLICY 13
6. REFERENCES 14
7. REGISTRATION OF CHANGES TO LOCAL NORMATIVE DOCUMENT 15

1. INTRODUCTORY PROVISIONS

PURPOSE

This Policy is the fundamental document intended to express the Company's position in information security, it defines a framework of views, principles and approaches in this area for ensuring security of the Company's business processes, creation of conditions of secure digital development of the Company and maintenance of conformity to requirements of the Russian legislation in this field, and also the applicable legislation of any other state where the Company carries out its operations.

This Policy is developed in accordance with the requirements of the Russian Federation legislation in the field of information security, taking into account applicable international standards and best practices.

SCOPE OF APPLICATION

This Policy shall be mandatory for employees of Rosneft Oil Company and subsidiaries of Rosneft with respect to which the Charters of the Subsidiaries, the shareholder and other agreements with partner companies do not set forth a special procedure for the Shareholders/ Participants to exercise their rights, including those to manage the Subsidiary.

This Policy does not apply to the organization and procedure for protection of information constituting state secrets.

VALIDITY AND AMENDMENT PROCEDURE

This Policy is a permanent local normative document.

The present Policy shall be approved, amended or deemed void at Rosneft by a resolution of the Rosneft Board of Directors and put into force at Rosneft by an Order of Rosneft.

2. GLOSSARY

2.1. CORPORATE GLOSSARY TERMS AND DEFINITIONS

AUTOMATED CONTROL SYSTEM (ACS)	A set of software and hardware tools designed to monitor and control process and/or production equipment (executive devices) and processes produced by them, as well as to manage such equipment and processes.
COMPUTER ATTACK	Actions aimed at implementation of threats of unauthorized access to IT asset, impact on it or resources of an automated information system with the use of software and (or) technical means.
IT SECURITY	A state of protection of the information environment ensuring its generation, use and development in the interests of the Company.
IT INFRASTRUCTURE	A set of information technology components, including hardware (data processing and storage systems, workplace equipment, peripherals, etc.), system software and engineering, networks, specialized premises.
IT SYSTEM	A complex of information contained in databases and information technologies and technical means ensuring its processing.
IT ENVIRONMENT	The collection of different information, together with the IT infrastructure and the entities that collect, use and disseminate information.
INFORMATION AND TELECOMMUNICATION NETWORK	A technological system designed to transmit over communication lines the information, access to which is provided by means of computer technology.
INFORMATION	Information shall mean any data (messages, data) regardless of the form in which they are presented.
IT-ASSET	An identifiable item or object related to information technologies, with a potential or actual value for the Company.
IT-LANDSCAPE	The collection of objects (information resources, means of information interaction and information infrastructure) that enter into information interaction with each other, as well as the information technologies that provide such interaction.
COMPANY	A group of legal entities of various forms of incorporation, including Rosneft Oil Company, for which the latter is the principal or prevailing (participating) entity
MOBILE DEVICE	Removable machine readable data carriers, hand-held computers and communication devices with data-processing features (personal laptop computers – notebooks, netbooks, tablet computers, and mobile phones, smart phones, smart watch/bracelets, digital cameras, sound recorders and other tools).

GROUP SUBSIDIARY (GS)	A business entity where Rosneft directly and (or) indirectly holds shares or equity stakes of 20 percent and more.
LEGAL ENTITY CONTROLLED BY ROSNEFT OIL COMPANY	A legal entity directly or indirectly controlled by Rosneft Oil Company entitled to directly or indirectly (via controlled legal entities) manage by virtue of participation in the controlled organization and/or under a trust management agreement, and/or partnership agreement, and/or agency agreement, and/or shareholder agreement, and/or any other agreement on exercise of rights certified by the controlled company's shares, and/or more than 50 percent of votes in the highest management body of controlled organization or the right to appoint (elect) a single executive body and/or more than 50 percent of members of the controlled entity's collegial management body.
SOFTWARE	A set of software systems for information processing and software documents necessary for the operation of these programs.
PRODUCTION MANAGEMENT INFORMATION SYSTEM	A collection of information technology components that automate the solution of planning and management tasks for various types of production activities and production processes.
INFORMATION SECURITY RISK	The combination of the probability of the threat to information security and the consequences of its implementation, which have a negative impact on the achievement of the Company's goals.
STRUCTURAL UNIT	A structural unit of Rosneft Oil Company or a Group Subsidiary with its individual functions, objectives and responsibility within its competencies determined by the Structural Unit Regulations.
INFORMATION SECURITY THREAT	A combination of conditions and factors that create a potential or actual risk of information security breach or IT asset security.
IT-ASSET VULNERABILITY	Deficiency (weakness) of the IT asset in general, which can be used to implement information security threats.
DIGITALIZATION	Applying break-through technologies transforming the operational processes through replacing of or adding to a human on the basis of a new quality analytics, artificial intellect, mobile and portable devices, robotization, integration process platforms.

2.2. ROLES

ROLES OF THE CORPORATE GLOSSARY

BUSINESS PARTNER	Existing and potential counterparties of Rosneft Oil Company and those of the Group Subsidiaries. *<u>Note:</u> Potential counterparties that do not currently have contractual relations with Rosneft Oil Company or a Group company are also considered to be business partners. Business partners also include public authorities (including tax authorities) and individuals (beneficiaries, founders). Potential business partners include business partners with whom Rosneft*

	Oil Company or the Group Subsidiary only plans to enter into contractual relations. Interaction with potential business partners is possible through accreditation, qualification assessment and price monitoring procedures.
CHIEF INFORMATION OFFICERS AND INFORMATION SECURITY SPECIALISTS	Leaders and/or employees of the structural unit of Rosneft Oil Company / Group Subsidiaries responsible for coordination, planning and organization of information security processes and their operational management.
THIRD PARTIES	Legal entities in which Rosneft Oil Company does not have the direct or indirect share in the charter capital, noncommercial organizations in whose management bodies there are no Company representatives, and also individuals who are not employees and are not members of the management bodies of Rosneft Oil Company and Group Subsidiaries.

ROLES FOR THE PURPOSES OF THIS DOCUMENT

COMPANY'S MANAGEMENT	Chief Executive Officer of Rosneft Oil Company, top managers of Rosneft Oil Company, sole executive bodies of the Group Subsidiaries.

3. INFORMATION SECURITY POLICY STATEMENT

This policy constitutes a document expressing Company's position with respect to information security. By adopting this Policy, the Company declares and undertakes to take all possible measures to protect employees, property, information, business reputation and business processes of the Company from the risk of damage, loss and damage resulting from the implementation of information security threats.

The Company's management is aware of the importance and need to promote and improvement of measures and means to ensure information security in the context of the development of Russian legislation and regulation of information security standards, as well as the development of information technologies used in the automation and digitalization of business processes and technological processes at production facilities. Compliance with information security principles will further strengthen the Company's competitive advantages, ensure compliance with legal, regulatory and contractual requirements and reduce image risks.

This Policy has been developed to establish principles that define general organizational and management approaches necessary to ensure and manage the Company's information security and protect the Company's interests from risks and threats to information security.

The Company's management is of the opinion that adherence to the principles, rules and regulations and information security requirements are, among others, part of the corporate culture. Compliance with the requirements of information security is an important condition for daily activities (including implementation of IT projects, development of digital initiatives, etc.), including joint work with Business partners. Each employee of the Company and its Business Partners is responsible for secure work with the corporate IT assets entrusted to him/her, computer equipment, mobile technical means, data carriers provided and processed by the Company.

Managers and information security specialists of the Company should perform their duties responsibly, being aware that the quality of their work directly affects the state of security of information, IT-assets, business and the Company's technological processes.

The Company employees shall be guided by this Policy in their professional activities, in intra-corporate cooperation, personal development and improvement of information security culture. The Policy discloses and supplements, if necessary, the rules defined in Rosneft's Code of Business and Corporate Ethics No. P3-01.06 P-01 in terms of information security principles.

3.1. COMPANY'S GOALS AND OBJECTIVES RELATED TO INFORMATION SECURITY

The Company's information security management are focused on achieving the following information security objectives:

- provision of a secure information environment to ensure the functioning and development of the Company's business processes;
- decrease in information security risk levels and threats to an acceptable level allowing to pursue sustainable digital development of the Company.

In order to achieve the above mentioned objectives, the following tasks need to be accomplished:

- ***ensuring information security of the Company's business processes in conditions of an increasing level of threats***, including ensuring operational monitoring and assessment of the state of security in the Company; improving the efficiency of protection against planned targeted computer attacks by intruders; improving information security of technological and production systems;
- ***application of new modern methods for secure digitalization of the Company***, including the organization of information security issues resolution in the implementation of digital solutions; organization of testing and application of new methods of information protection from modern threats, including through interaction and partnership with leaders of information security industry; ensuring application of secure digital technologies in implementation of domestic developments and development of the Company's own competitive corporate software;
- ***compliance with state requirements in the field of information security*** by ensuring a specified level of information security of IT assets in accordance with the requirements of the current legislation of the countries where the Company operates.

3.2. INFORMATION SECURITY OBJECTS

As part of ensuring information security, the Company's objects of protection are information processed in the Company, regardless of the form of presentation; IT assets, including but not limited to the following list:

- automated work places, information-processing equipment and mobile devices;
- information systems, data storage systems, software and particular technical solutions;
- Automated Control System, metrology and industrial automation systems, including measuring and loading systems;
- IT infrastructure, information and telecommunications networks, signal communication systems;
- IT services rendered by the Company or in the Company's interests;
- solutions related to digitalization of business and process (production) processes.

3.3. MAIN PRINCIPLES OF INFORMATION SECURITY MANAGEMENT AND ASSURANCE

The Company's activities in the area of information security are carried out in compliance with the following basic principles[1].

Focusing on the Company's strategy - strategic initiatives on information security are developed and implemented in accordance with the overall strategy and goals of the Company's development, taking into account corporate strategies in the field of information technologies and in the field of industrial automation, metrology and quality control.

Centralization of management functions - the principle is the possibility of taking managerial decisions related to information security at the Company's level through operational monitoring (of the Company's IT landscape and the external information environment) and assessment of the information security status; implementation of centralized management of strategic information security initiatives; control over the implementation of measures to develop information security; creation and development of centralized solutions related to information security; creation and development of centralized solutions related to information security.

Proactive approach and risk management - is based on monitoring, analysis and assessment of emerging, current and future IS risks and threats to information security (including the study of technologies used by intruders) in order to take timely and conscious preventive measures to prevent computer attacks and prevent damage to the Company.

Standardization and unification - means development and replication in the Group Subsidiaries of the standardized requirements and approaches, standard technical solutions and elements of information security assurance architecture for unification of means and methods of solving the same problems; interfaces of information security management systems.

Import substitution - involves reduction of risks of unfavorable external market conditions due to the focus on domestic solutions, means and services while ensuring information security in the Russian Federation.

Resource support - means the need to allocate targeted funding to ensure and develop the Company's information security and maintain the required organizational structure.

Legitimacy and compliance - the Company's information security activities are based on compliance with the requirements of the regulatory legal acts of the Russian Federation and national legislation of the countries where foreign Group Subsidiaries operate.

Improvement of information security culture - declares the need not only to inform all employees of the Company, its Business Partners and third parties using the Company's IT assets about information security requirements, but also to develop skills of acceptable information handling and secure work with the Company's IT assets.

Development of competencies and professionalism - the principle means the need to constantly develop the competencies and practical skills of information security specialists under conditions of continuous change of IS risks, landscape of used information technologies and techniques of

[1] These principles have been developed taking into account international standards and practices in the field of information security, including COBIT 5 for Information Security; ITIL: 2011 Service Design; ISO/IEC TS 19249:2017.

potential violators. Ensuring information security in the automation of technological and production processes requires competence and knowledge in the areas of industrial automation and metrology.

Knowledge accumulation and exchange of experience - it is necessary to accumulate knowledge and share experience in the course of practical activities to ensure information security (in monitoring and responding to computer attacks, in implementing and operating technical solutions, in auditing information security, etc.).

Information security as an integral property of an IT asset is a principle that is as follows:

- Information security requirements shall be taken into account at all stages of the IT asset life cycle, regardless of the level of confidentiality of the information processed in the IT asset;
- development of software products in the Company's interests is carried out using methods of secure software development;
- preferable are IT assets with the greatest coverage of information security requirements with built-in features (all other characteristics being equal);
- built-in information security features must be configured and used when operating IT assets, including software and hardware, automated control systems, etc.;
- compliance of the acquired/implemented IT asset with the required information security level is confirmed in accordance with the existing procedures, taking into account the requirements of the applicable legislation.

Information security as an integral property of IT services - means that IT-services offered and provided to the Company or in the interests of the Company must be designed and implemented in accordance with information security requirements.

Compatibility - refers to the selection of components for information security in a way that ensures their mutual system compatibility at the information, software, electromagnetic and operational levels, as well as compatibility with the used IT solutions, information technologies and with solutions for automating the Company's technological and production processes.

Reliability - using information security components and tools that meet reliability, availability requirements and serviceability.

Adequacy and validity of decisions - measures taken in the Company and the information security tools used are effective, efficient and are proportionate to the amount of IS risks and threats to information security that affect the Company's goals.

Comprehensiveness - the application of any available legal methods, means and measures (including legislative and regulatory, organizational and administrative, software and hardware, engineering and physical) aimed at reducing IS risks, preventing threats to information security and preventing damage to the Company, its Business Partners and employees.

Segregation and minimization of duties - means that critical (final) operations are performed only by means of segregation of actions (for example, algorithmic segregation, temporary or resource segregation - including by two employees). The elimination of a sole critical operation can be organized at the level of organizational measures and/or software and hardware by delegating authorities or user role. The software and hardware method of segregation of duties is preferable over organizational. There should be a control of realization of principles of critical authorities differentiation in information systems and in ACS, restriction of access rights, depending on a level

of the agreed authorities. The authorities should be minimally sufficient to enable the person to perform his or her official duties or fulfil contractual obligations. If necessary, there should be control of authorities conflict - organizational, as well as software and hardware.

Continual improvement of information security - providing constant improvement of existing practice and improvement of means and methods of management and maintenance of information security on the basis of results of information security audits, monitoring of information security systems functioning, analysis of changes in methods and means of computer attacks, analysis of regulatory requirements and existing advanced domestic and foreign practices in this area.

4. LIABILITY FOR BREACHES OF INFORMATION SECURITY

Employees of the Company shall comply with information security requirements and rules when working with information and IT assets of the Company and its Business Partners.

High corporate standards and information security rules are mandatory for all Company employees without exception and must be taken into account in their relations with Business Partners.

The Company's management assigns responsibility to heads of structural units, representative offices and branches of Rosneft Oil Company / Group Subsidiaries for organization of daily activities and allocation of necessary resources to ensure information security as an integral part of business and production processes; for timely identification of significant IT assets, appointment of those responsible for IT assets and management of access to them; for submission of established information security requirements to the Company's employees and Businesses.

When using the Internet, social networks and messengers, e-mail, other telecommunication and mobile technical means, the Company's employees are advised to exercise caution and self restraint in order to avoid personal security risks and to avoid unintentional leakage of working information. The rules of external communications are established by the Code of Business and Corporate Ethics of Rosneft, № P3-01.06 P-01 and the Information Policy of Rosneft № P3-01.04 P-01 Yul-001 / internal documents of the Group Subsidiaries in the field of information policy.

Each employee of the Company bears disciplinary, civil, administrative and criminal responsibility for failure to comply with information security requirements in accordance with the legislation of the Russian Federation.

Employees of foreign Group Subsidiaries are responsible in accordance with the current legislation of the country where they operate.

Employees of Business Partners who use corporate IT assets, as well as the information provided by the Company, are responsible in accordance with the contractual relations with Rosneft Oil Company or the Group Subsidiary, as well as applicable law.

5. AWARENESS AND COMMUNICATION OF POLICY

This Policy is a public document.

Rosneft Oil Company and the Group Companies also communicate this Policy to their Business Partners and Contractors and interact with them subject to the provisions of this Policy.

6. REFERENCES

1. COBIT 5 for Information Security.

2. ITIL 2011: Service Design. ISBN 9780113313051.

3. ISO/IEC TS 19249:2017 Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications.

4. Rosneft's Code of Business and Corporate Ethics, No. P3-05.02 P-01, Revision 1.00 approved by Rosneft's BoD resolution on 05.06.2015 (Minutes No. 35 of 05.06.2015), put into force by Rosneft order No. 428 of 28.09.2015.

5. Rosneft's Information Policy № P3-01.04 P-01 Yul-001 version 3.00 approved by the Rosneft Board of Directors on 15.11.2017 (Minutes № 6 dated 17.11.2017), put into force by Rosneft's Order No. 53 dated 30.01.2018.

7. REGISTRATION OF CHANGES TO LOCAL NORMATIVE DOCUMENT

Table1
List of changes of the Company Policy

VERSION	TYPE AND NAME OF DOCUMENT	DOCUMENT NUMBER	APPROVAL DATE	EFFECTIVE DATE	DOCUMENT DETAILS
1	2	3	4	5	6
1.00	Company Policy «Information and Technical Security Concept of Rosneft Oil Company»	PZ-11.1	14.03.2008	14.03.2008	Rosneft's Order № 124 dated 14.03.2008